Proceedings of the Third International Conference on Smart Systems and Inventive Technology (ICSSIT 2020)
IEEE Xplore Part Number: CFP20P17-ART; ISBN: 978-1-7281-5821-1

Biometric Based Smart ATM Using RFID

Gokul.S, Kukan.S, Meenakshi.K, Vishnu Priyan S S, Rolant Gini J, M.E.Harikumar
Department of Electronics and Communication Engineering
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham, India
gokulsridharan1999@gmail.com, s.kukan77@gmail.com, meeru.krishh@gmail.com, vishnu32510@gmail.com, j_rolantgini@cb.amrita.edu, me_harikumar@cb.amrita.edu

***Abstract* — In the present world, the usage of ATM to withdraw cash has increased. At the same time, theft and robbery cases have also been increased that calls for the need for much-secured ATM that provides additional features for security. In this work, the aim is at security-based smart ATM which functions based on RFID and fingerprint authorization for its access. The RFID number and fingerprint details are obtained from the user after which the recognized card number, authorization status, and location of access are passed on for checking its authenticity with the database details. Once the information is validated with the retrieved database details then the corresponding account holder gets the message if the authorization is valid or not. The location, time, and date of the access are also informed to the account holder. Additionally, this enhances the security by placing vibration and flame sensors which immediately notify in case of fire and breakage. To achieve complete security, the face of the person accessing the ATM card is also recorded – using a camera – in the machine with time and date of access that could be used in case of suspicion.**

Keywords—IoT; RFID; esp8266; microcontroller; fingerprint sensor; embedded system; signal processing.

I. INTRODUCTION

An Automated Teller Machine (ATM) is a computerized machine that provides customers of the banks the facility of accessing their accounts for dispensing cash and to carry out other financial and non-financial transactions without the need to visit the bank branch. ATM's were first used in London in 1967, and after 50 years, these machines were introduced nationwide. The growth of ATM development is briefed in Table I [1].

ATM points are conveniently located at multiple locations. ATM of any bank can be accessed to withdraw cash in 24x7 hours, 365 days a year. If one is travelling overseas, then the card can be used to draw currency of the country an individual is travelling to, from the ATM. The use of an ATM is restricted only to the person who knows the PIN (Personal Identification Number). The single most benefit of the ATM is to save time in driving down to the branch and one need not has to waste time waiting in the queue to perform transactions. The ATM facilities provide the option of banking instantly for various transactions. Apart from cash withdrawal and checking account balance, modern ATMs are used to open a fixed deposit with a bank, recharge mobile, pay income tax, deposit cash, pay the insurance premium, apply for a personal loan, transferring cash, paying the bill, booking railway ticket, etc.,

TABLE I. TIMELINE OF AN ATM – A BRIEFING

Period	Development
1988 – 1994 (The starting period)	Cash deposit and cash withdrawal
1995 – 1999 (Initial developments)	Mini statements and balance in quiry
2002 – 2004 (Extended developments)	Chequebook request, Fund transfers, and Touch screen facilities
2004 – 2006 (Third-party services)	Railway and Airway ticket booking. Bill payment (like electricity, Broadband..). Recharging for mobile phone
2007 onwards	Customized ATM services

As there are many ATM centres across India, each centre must be ensured with security as the number of ATM theft cases are increasing day by day. As a result, in addition to security officers at the ATM, more reliable security methods are necessary. Shockingly, nearly 50 theft cases have been reported just between January 2020 and 16 April 2020 at various ATM centres across India; a few of which also include uprooting of the ATM [2]. Therefore, this project mainly aims to build a secure, easily accessible, and safe ATM.

II. THE EXISTING SYSTEM OF THE ATM

The current ATM system provides two types of services. The former one provides the customer with the cash requested and sends a message with a report of the amount taken and account balance. The latter one is more advanced to accept the deposit from the user, provides credit card payment facilities, and sends a message to the user about the transaction and account information.

The existing system of ATM has been briefed in Fig. 1. The input to the ATM is recognized through the input devices such as card reader and keypad. The card reader is an input device that is used to read data from the card which identifies the user's card number. The card is either swiped or pressed on the card reader that captures the account information once a connection is established with the magnetic strip on the backside of the ATM card. This information is passed to the host server that uses the data to get details about the cardholder. To get details from the user, currently have a keypad which contains around 48 keys that are interfaced with the processor. The card is recognized using a Personal Identification Number (PIN). After the PIN is authorized, the user can choose any service provided by the ATM through the

keypad. To ensure security, every card has a unique PIN and the PIN is sent to the host processor in the encrypted form.

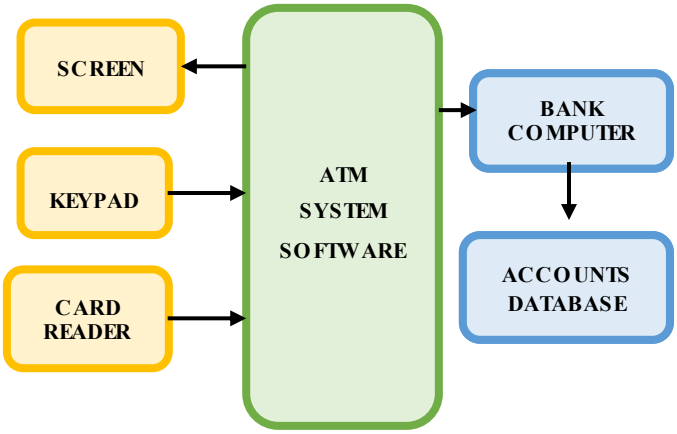

Fig. 1. Block diagram of the existing system.

A. *Merits of an existing ATM system*

- The system provides a message to the cardholder as soon as the transaction happens.
- The system provides flexibility that the user needn't come to the ATM instead anyone who knows the card's PIN can access the card.
- Every card has a unique PIN.
- The PIN is sent to the processor in an encrypted form.

B. *Demerits of an existing ATM system*

- Criminals can fit small cameras to ATMs that record account details and personal identification numbers that increase the risks of fraud and robbery.
- The user doesn't get any message about the unauthorized access of the card.
- The user doesn't get information about the location of access to the card in the case of theft.
- The face of the person accessing the ATM is stored as video in CCTV which needs more storage space.
- Import details like card number, CVV are displayed on the ATM card that supports misusing the card.

Throwing light to the various scenarios referred, the developments in the existing ATMs are required on using alternate methods for authentication instead of a PIN [3], [4], sending alert messages [5] on detecting vibration on the machine, having cameras to record people who are accessing the ATM [6]. This paper mainly aims at using RFID tag and fingerprint as the input to the ATM. Since the cardholder gets a message regarding the authentication status, location of the ATM, date, and time of access regardless of if the access is valid or not which helps the cardholder get information about his/her card being misused. In addition to this, the vibration and flame sensors prevent robbery and fire accidents by alerting the respective departments by giving a message about the incidents. It is important to note that the methods for sending messages are cost-efficient in this project. Moreover, using a camera to capture the face of the user at the ATM helps reduce unwanted storage space as required by that of CCTV cameras.

III. THE PROPOSED SYSTEM OF THE ATM

The proposed system is a microcontroller-based ATM in which normal cards are replaced with RFID cards that contain the card number of the user. Instead of using the PIN, the fingerprint of the user is used for authorization. Hence if the person is in the vicinity of ATM, his/her card is scanned by the RFID scanner and the system waits for the valid fingerprint of the corresponding card. If a valid fingerprint is recognized by the fingerprint sensor of the ATM, a message will be sent to the phone number, registered to the card, stating that "The access is granted". On the other hand, if an invalid fingerprint is recognized, the user of the corresponding card gets a message stating that "Access not granted! Someone has tried to access this card". Regardless of if the access is granted or not, the cardholder also gets details about the time, date, and location of the access. To minimize the storage of unwanted video feed, the images of the people inside ATM are saved in the database through a camera that helps the respective bank and the cardholder in case of theft at the ATM. In case of fire in the ATM, the proposed system automatically sends a message to the fire station along with the GPS coordinates of the ATM. Moreover, if someone tries to break the ATM, the system automatically sends a message to the police station along with the GPS location of the ATM which is essential [7]. Thus, the proposed system combines a lot of required aspects in the field of ATM's security to help the bank and ensures security at the ATM. The block diagram in Fig.2 shows the working of the proposed system.

The proposed system uses hardware components like RFID scanner and cards, fingerprint sensor [8], GPS module, NodeMCU, flame sensor, and vibration sensor. It has used software platforms including Arduino for processing the received input from the sensors, MIT app inventor that creates an application for tracking the changes in the values of the sensor readings, to send messages and firebase for cloud storage.

The main reason for which NodeMCU is used is that it has a built-in WiFi module in it that helps to send the necessary values to the cloud database, in this case, it is the firebase. The MFRC522 based RFID reader module used as the user's card and the corresponding card reader uses electromagnetic fields to transfer data over a short distance with a frequency of 13.56MHz. An R307 fingerprint module is used for obtaining the fingerprint as a password for authentication from the user. The fingerprint processing mainly includes two elements namely enrolment and matching. In fingerprint enrolling, every cardholder requires to place the finger twice on the sensor that the system checks the finger images to process and generates a pattern of the finger. The enrolled fingerprint is stored. In matching, during the ATM access, the user places the finger on the optical sensor after which the system produces a pattern of the finger and compares it with those fingers enrolled in the finger library templates.

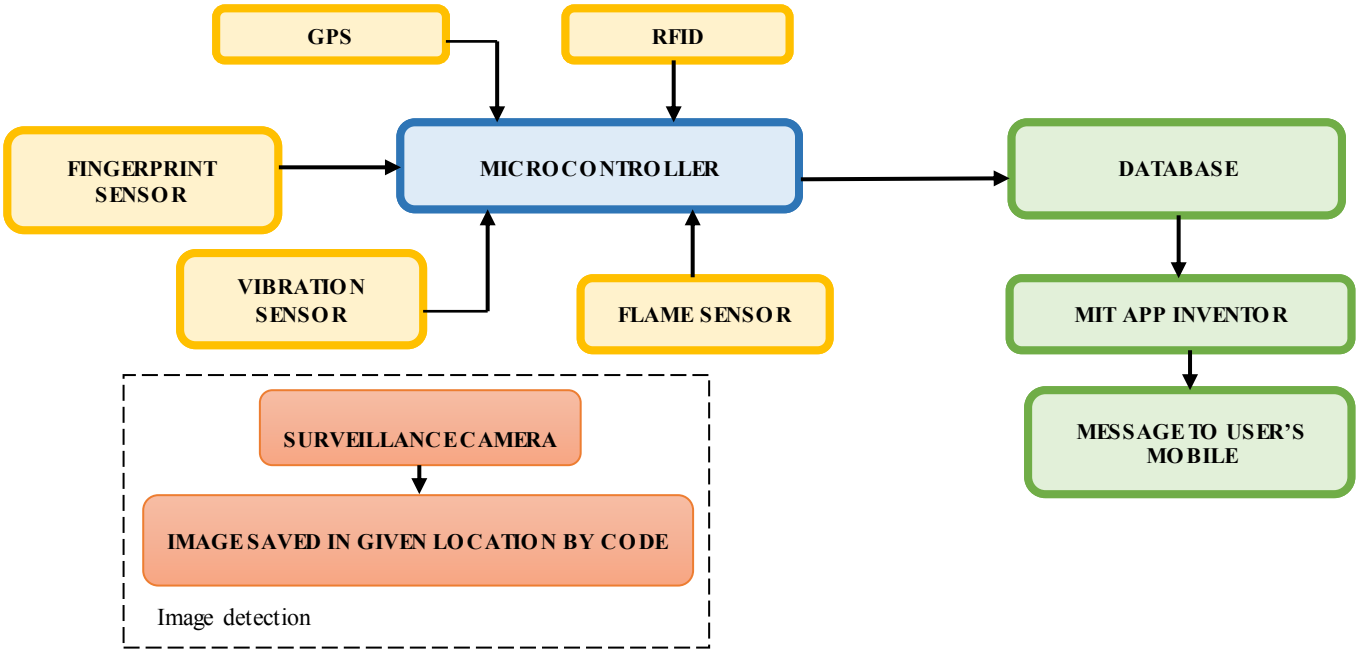

Fig. 2. Block diagram of the proposed system.

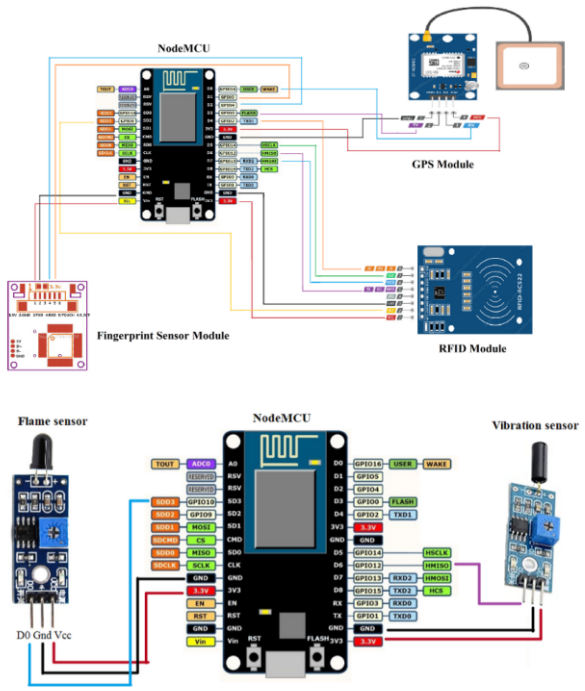

Fig. 3. Circuit diagram of the proposed system

In addition to this, a GPS module is used to get details like the location of where the transaction has happened, date, and time of the access. The main advantage of sending the longitude and latitude of the ATM to the user is that the location of the ATM is known exactly and it avoids confusions in case if there are many ATM centres at the same location. Firebase is the cloud database used in this project where the vital parameters like card details, authorization status, location of the ATM, time, and date of access are updated from the ATM. One of the main purposes of using the database is to get the details about the recent transaction and send messages to the corresponding cardholder. A mobile application was created using MIT App Inventor- a web application development environment in which the values from the firebase are retrieved for sending messages to the cardholder with relevant details. Moreover, for taking actions against accidents and thefts, flame and vibration sensors are used to ensure the safety at the ATM. Further, Python has been used for applying image processing techniques that capture the images of the faces of the users using the ATM. The stored images are pushed to the database for future verification. By recognizing the image and pushing it to the database, the security of the ATM is enhanced as there is an increase in ATM card thefts and fingerprint frauds

IV. Results and Discussions

When the circuit is set as shown in Fig.3, the code is fed into the microcontroller. Assuming that there are RFID cards with card numbers in them and their respective fingerprints are stored for future authorization, an app is built to keep track of the values such as RFID card number, user ID, location of the access, access status (if the authorization is valid or not), etc. This application was built by a tool named "MIT app inventor". This is the tool that is used to send messages to the user after the access of the card at the ATM.

Fig. 4. The developed mobile application's icon/logo.

The start-up icon of the developed mobile application has been shown in Fig. 4. The home page and its orientation of the application can be seen as shown in Fig.5. When a transaction or an attempt for a transaction is made, the respective values get updated in the firebase (the database used) which is retrieved through the developed android application Fig.4. Following this, the respective values for RFID card number, user ID, location of the access, access status, flame, and vibration sensor status are updated in the application replacing the text of the corresponding labels. Each label stands for one ATM.

Fig. 5. Home page of the application.

Four possible cases can happen in the system developed in real-time working as shown in Table II. The first case happens when a user uses or tries to access through an invalid card. In this case, the ATM displays it as an invalid user. The second case happens when the user accesses the system using a valid card and give in the corresponding valid fingerprint for the card. In this case, the access is granted and the values of the RFID card number, location, and time of access are updated in the Firebase and they are retrieved through the application. A message is sent to the registered phone number of the cardholder of the respective card stating that "the access is authorized" along with GPS coordinates of the ATM where the card was accessed and other credentials as shown in Fig.6 and Fig. 7.

TABLE II. TEST CASES

Scenarios	Case 1	Case 2	Case 3	Case 4
RFID Card	Invalid	Valid	Valid	-
Fingerprint	-	Valid	Invalid	-
Message	Not Sent	Sent	Sent	Sent

The third case happens when the access for the system is given by a valid card but it is given an invalid fingerprint for the respective card. The access is not granted in this case as the system expects the corresponding fingerprint for the card registered previously. The values for the RFID card number, location, and time of access are updated in the Firebase and are retrieved through the application. The response in the Firebase & IDE has been shown in Fig. 8 for the denied case. A message is sent to the registered phone number of the cardholder stating that the "access is denied" along with the GPS coordinates of the ATM where the card has been tried for access and other credentials like time, date, etc. as in the Fig. 9.

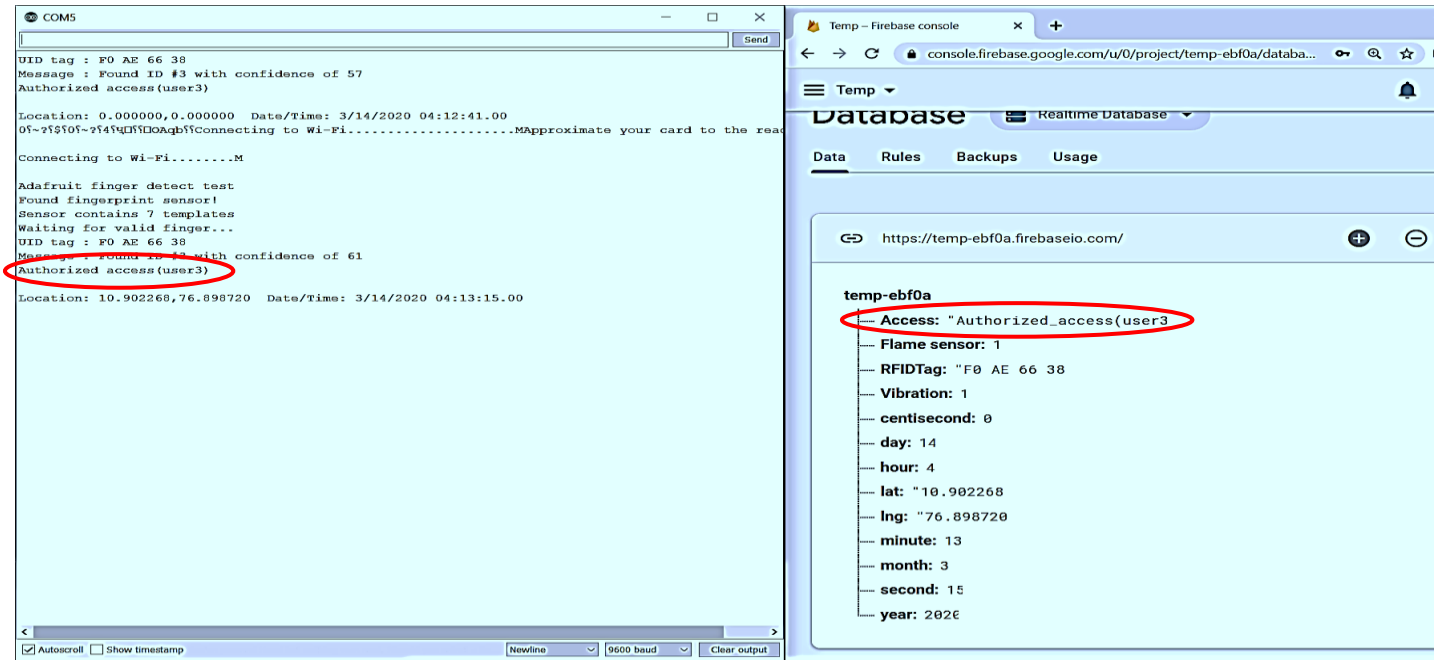

Fig. 6. Firebase & IDE display for an authorized case. The authorization has been indicated with the red colour circles on both platforms.

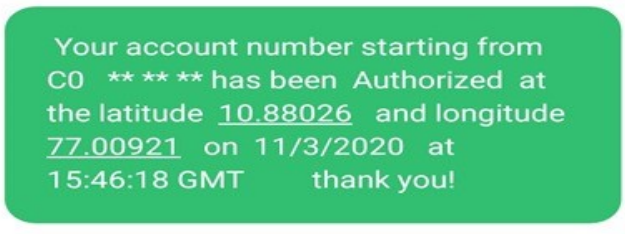

Fig. 7. Message received by the cardholder in an authorized case

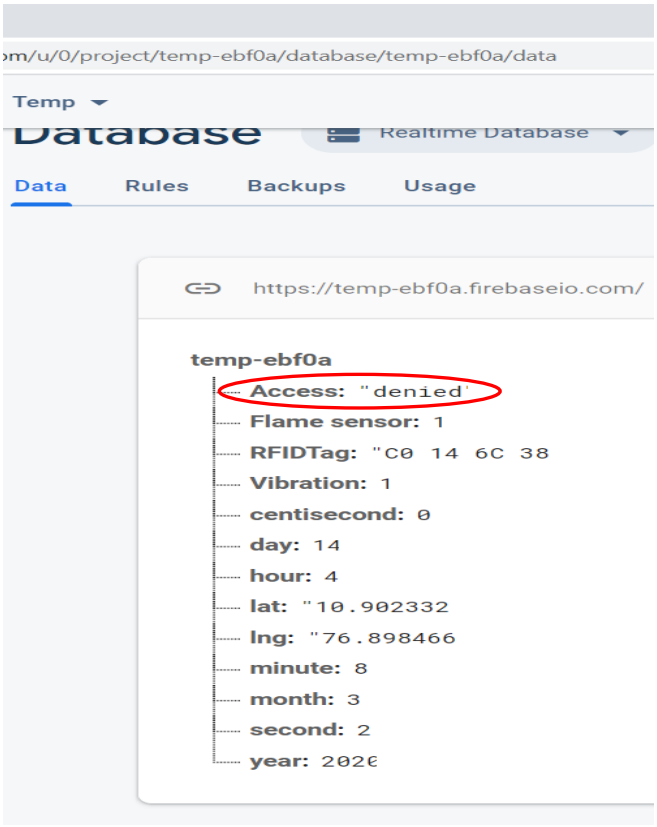

Fig. 8. Firebase data for access denied case indicated by a red circle.

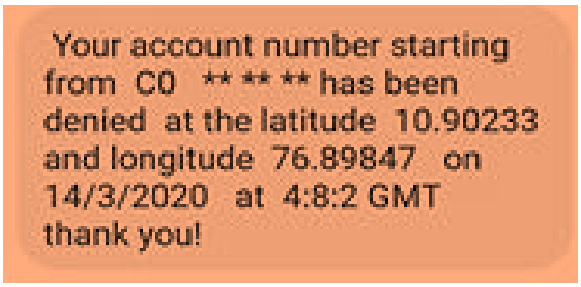

Fig. 9. Text message received by the cardholder in a denied case.

The fourth case is to ensure safety at the ATM by placing flame and vibration sensors. In case, if someone tries to break or damage the ATM, a message is sent to the police station about the action with the GPS location of the ATM as shown in Fig. 10. In case of fire, a message is sent to the fire station with the GPS location of the ATM, as shown in Fig.10, for immediate actions to prevent it from causing heavy damages.

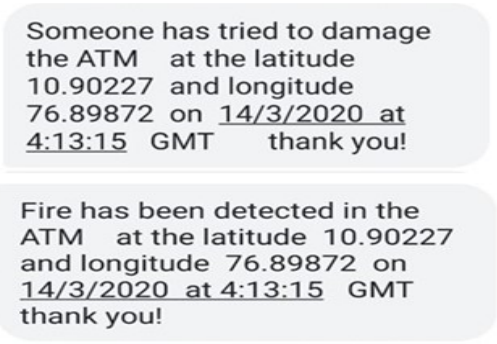

Fig. 10. Text message received by the police station and fire station.

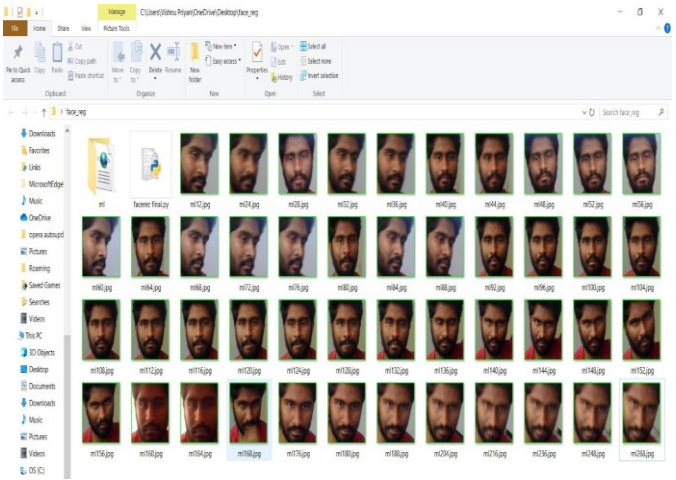

Fig. 11. Database for users accessing the ATM.

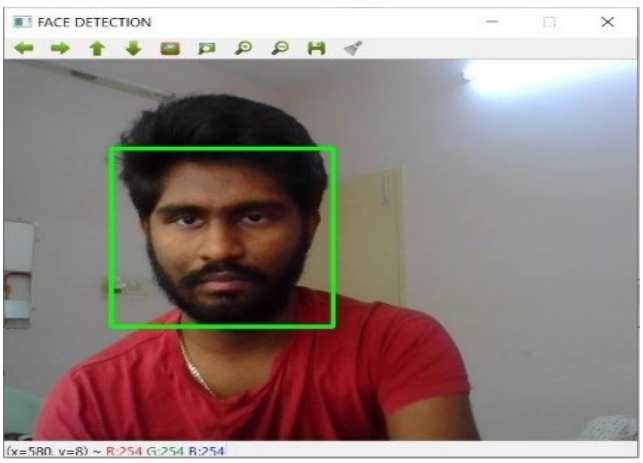

Fig. 12. Capturing the user's face while accessing the ATM.

To keep track of people entering the ATM, a signal processing technique for capturing the face of that person is used. The image of the CCTV placed in the ATM takes more storage space. To reduce storage space, the python was used for tracking the images of the faces of various people who use the ATM. The camera fitted in the ATM tracks the people who

are using the ATM. To implement this, the "OpenCV" module in python is used. Haar feature-based Cascade classifier is used in the code which uses object detection algorithm to identify objects in an image or a video. When the program is executed, the camera searches for a face with the help of the facial features using the classifier. Once the face is recognized, it is flipped, reshaped and highlighted. A rectangular box is drawn around the face and is pushed to the database. The capturing of the face of the user is shown in Fig.11 and the location where all the users' images are saved is shown in Fig.12. Thus, these specifications pave the way for an ATM system to be effective, secure, and easily accessible.

V. CONCLUSION

Thus this proposed system used the RFID card and the user's fingerprint for authorization. In the case of multiple accounts, different RFID cards can be used for each bank accounts. The card closest to the proximity of the card reader will be considered for the current operation. It enhances the security by sending messages to the cardholders for the card holder's register number about the location, date, and time through the GPS, regardless of if the transaction is valid or not. Also, a camera that is set regularly checks who is trying to access the card in the ATM that helps in cases of fraud. It prevents accidents and robbery as the sensors that are fit immediately alert the respective departments. The effective results for the prototype verify the proposed system for smart ATM.

The proposed system is just a prototype of an ATM system in which money transferring facilities can be added to be implemented at the ATM. In addition to sending the user the GPS location of the ATM, the amount of cash withdrawn, the image of the face of the user can also be sent. To increase the security against the theft and accidents at the ATM, more accurate sensors for fire detection and damage detection can be inserted [9], [10]. Since the fraud in fingerprint recognition has increased, to ensure security towards this issue in the proposed system, extra tiers of safety measure like face detection, iris scanner, OTP generation can be added.

VI. REFERENCES

[1] Hota, Jyotiranjan. (2013). Growth of ATM Industry in India. CSI Communications. 36. 23-25.

[2] The Times of India, "Atm Crimes". Available: https://timesofindia.indiatimes.com/topic/Atm-Crimes [Accessed: May 08,2020].

[3] Christiawan, B. A. Sahar, A. F. Rahardian and E. Muchtar, "Fingershield ATM – ATM Security System using Fingerprint Authentication," International Symposium on Electronics and Smart Devices (ISESD), Bandung, 2018, pp. 1-6 J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[4] S. Hazra, "Smart ATM Service," 2019 Devices for Integrated Circuit (DevIC), Kalyani, India, 2019, pp. 226- 230.

[5] S. Sankhwar and D. Pandey, "A Safeguard against ATM Fraud," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 701-705, doi: 10.1109/IACC.2016.135.

[6] K. Archana, P. B. Reddy and A. Govardhan, "To enhance the security for ATM with the help of sensor and controllers, "2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 1012-1015, doi: 10.1109/ICECDS.2017.8389590.

[7] V. M. E. Jacintha, S. J. Rani, J. G. Beula and J. J. Johnsly, "An extensive resolution of ATM security systems," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), Chennai, 2017, pp.934-938, doi: 10.1109/ICONSTEM.2017.8261340.

[8] Rhydo Labz. R30X Series Fingerprint Identification Module User Manual. Available: https://www.rhydolabz.com/documents/finger-print-module.pdf. [Accessed: May 08,2020].

[9] P. A. Paresh and Dr. Latha Parameswaran, "Vision-based algorithm for fire detection in smart buildings", in Lecture Notes in Computational Vision and Biomechanics, vol. 30, Springer Netherlands, 2019, pp. 1029-1038.

[10] V. Ashokan and Murthy, O. V. R., "Comparative evaluation of classifiers for abnormal event detection in ATMs", in 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT 2017, 2018, vol. 2018-January, pp. 1330-1333.